ELSEVIER
Available online at www.sciencedirect.com
SCIENCE DIRECT®
European Journal of Combinatorics 27 (2006) 1042–1053
European Journal of Combinatorics
www.elsevier.com/locate/ejc

On groups with the Lohse property

David Meier

Pilgerweg 1, 8044 Zurich, Switzerland

Accepted 23 September 2004
Available online 10 May 2005

Abstract

A finite group has the Lohse property if the rows and columns of its Cayley table can be arranged in such a way that entries in diagonally adjacent positions are different. In this paper we determine the groups with the Lohse property completely: all finite groups except the groups of order less than or equal to four and the quaternion group have the Lohse property. The decisive properties are that the group has a generating system, which is closed under taking inverses, of size less than half the order of the group, and the existence of a Hamilton cycle in the Cayley graph for certain generating systems of the group.

1. Introduction

A latin square is an $n \times n$ matrix with entries from a set with n elements $\{e_0, e_1, \ldots, e_{n-1}\}$ such that every element occurs exactly once in each row and column. We are interested in latin squares in which diagonally adjacent elements are different in the stronger sense of Definition 1.

Definition 1. The latin square $(a_{i,j} | 0 \le i, j \le n-1)$ is in Lohse form if the following inequalities hold.

$$a_{i,j} \neq a_{i+1,j+1} \qquad \text{for } 0 \le i, j < n,$$
$$a_{i,j+1} \neq a_{i+1,j} \qquad \text{for } 0 \le i, j < n,$$

where addition of indices is performed modulo n.

E-mail address: davidmeier@bluewin.ch.

doi:10.1016/j.ejc.2005.04.006

Remark on *addition modulo n* for indices:

We will throughout the paper use *addition modulo n* for the *indices* of a sequence of size n or a square of size $n \times n$ to avoid special treatment of borders and corners.

This means for example that we get in the Definition 1 above for $i = n-1$ or $j = n-1$ the following inequalities for the first and last row and the first and last column and for opposite corners.

$$\begin{array}{lll} a_{i,n-1} \neq a_{i+1,0} \quad \text{and} \quad a_{i,0} \neq a_{i+1,n-1} & \text{for } 0 \leq i < n, \\ a_{n-1,j} \neq a_{0,j+1} \quad \text{and} \quad a_{n-1,j+1} \neq a_{0,j} & \text{for } 0 \leq j < n, \\ a_{n-1,n-1} \neq a_{0,0} \quad \text{and} \quad a_{n-1,0} \neq a_{0,n-1}. & \end{array}$$

The definition of Lohse form is therefore invariant under cyclic permutations of rows or columns.

Two latin squares are called isotopic if one can be transformed into the other by rearranging rows, rearranging columns and renaming elements; see [2].

Definition 2. A latin square has the Lohse property if it is isotopic to a latin square which is in Lohse form.

The multiplication table or Cayley table of a group G is a latin square.

Definition 3. The finite group G has the Lohse property or is a Lohse group, if its Cayley table has the Lohse property.

Put in a different way, the group G is a Lohse group, if there exist enumerations of its elements $h = (g_0, g_1, \ldots, g_{n-1})$ and $v = (g_{\pi(0)}, g_{\pi(1)}, \ldots, g_{\pi(n-1)})$, where π is a permutation of $0, 1, \ldots, n-1$, such that the Cayley table with h as horizontal border and v as vertical border and entries $g_{i,j} = g_{\pi(i)} g_j$ is in Lohse form:

	g_0	g_1	$\cdots$	g_{n-1}
$g_{\pi(0)}$	$g_{0,0}$	$g_{0,1}$	$\cdots$	$g_{0,n-1}$
$g_{\pi(1)}$	$g_{1,0}$	$g_{1,1}$	$\cdots$	$g_{1,n-1}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$g_{\pi(n-1)}$	$g_{n-1,0}$	$g_{n-1,1}$	$\cdots$	$g_{n-1,n-1}$

The simplest example of a Lohse group is the cyclic group of order five. A Cayley table in Lohse form is the following.

	0	1	2	3	4
0	0	1	2	3	4
2	2	3	4	0	1
4	4	0	1	2	3
1	1	2	3	4	0
3	3	4	0	1	2

A series of paintings, the so called ‘serial orders’, of the renowned Swiss artist R.P. Lohse, who lived from 1902 to 1988, [6] or [4], are squares with $n \times n$ fields, colored by n colours, which are latin squares such that each field with a given colour is completely isolated from the other fields with the same colour, i.e. where diagonally adjacent fields are differently coloured. My father, the group theorist H. Meier-Wunderli, studied the 'serial orders' of R.P. Lohse and found that most of them are Cayley tables of cyclic groups. This led him to study other groups with respect to this property, which he called the Lohse property, and he noticed that the quaternion group is not a Lohse group. This was the starting point of our investigation. The main result of the paper is the following: all groups except the groups of order less than or equal to four and the quaternion group are Lohse groups.

Latin squares are important as experimental designs; see for example the corresponding chapter in [2]. The property of having different entries in diagonally adjacent positions does not seem to be of direct importance, even if other properties, which imply it, occur in the literature. For example, a latin square, in which every element occurs also in every of the n left and right diagonals, a so-called Knut Vik design, see [5], is necessarily also in Lohse form. The Cayley table of the cyclic group of order five above is also a Knut Vik design.

The organization of the paper is the following. In Section 2 we shall formulate an equivalent condition for a group to possess the Lohse property (cf. Theorem 1). This alternative approach is based on the investigation of consecutive quotients that are obtained from a cyclic ordering of the group elements. In Section 7 we shall see how this approach can be used to verify the Lohse property when we know that an associated system of generators yields a Cayley graph with a Hamilton cycle. Since Hamilton cycles are presently known to exist only under certain conditions the method can be applied only to some group orders. Many groups that are not covered are considered in Sections 3–6, where one can find a number of direct constructions. The final result is obtained by combination of both approaches.

2. Equivalent conditions

The main result of the section is a condition, that is equivalent for a group G to the Lohse property, but is easier to apply. If $e = (g_0, g_1, \ldots, g_{n-1})$ is an enumeration of the elements of G, we use the following notation and definitions.

Definition 4. The set of quotients $Q(e)$ of the enumeration e is the set of all distinct elements of $g_i^{-1}g_{i+1}$ for $0 \le i < n$ and their inverses.

Definition 5. The inverse of e is the enumeration $e^{-1} = (g_0^{-1}, g_1^{-1}, \ldots, g_{n-1}^{-1})$.

Definition 6. Two rows $r_1 = (g_{1,0}, g_{1,1}, \ldots, g_{1,n-1})$ and $r_2 = (g_{2,0}, g_{2,1}, \ldots, g_{2,n-1})$ are said to have cyclically different entries in diagonally adjacent positions if the following inequalities hold:

$$\begin{aligned} g_{1,j} &\neq g_{2,j+1} && \text{for } 0 \le j < n, \\ g_{1,j+1} &\neq g_{2,j} && \text{for } 0 \le j < n. \end{aligned}$$

The following lemma establishes a connection between equal elements in diagonally adjacent positions and quotients of consecutive elements in the horizontal and vertical borders of the group table.

Lemma 1. *Let G be a group of order n and π a permutation of $0, 1, \ldots, n-1$ and $h = (g_0, g_1, \ldots, g_{n-1})$ and $v = (g_{\pi(0)}, g_{\pi(1)}, \ldots, g_{\pi(n-1)})$ two enumerations of the elements and let $(g_{i,j} | 0 \le i, j \le n-1)$ be the group table with h as horizontal and v as vertical border and $g_{i,j} = g_{\pi(i)} g_j$ for $0 \le i, j < n$.*

Then (a1) *and* (a2) *are equivalent and* (b1) *and* (b2) *are equivalent for fixed i and j:*

(a1) $g_{i,j} = g_{i+1,j+1}$.
(a2) $g_{\pi(i)}^{-1} g_{\pi(i+1)} = g_j g_{j+1}^{-1}$.
(b1) $g_{i,j+1} = g_{i+1,j}$.
(b2) $g_{\pi(i)}^{-1} g_{\pi(i+1)} = g_{j+1} g_j^{-1}$.

Proof. We consider a section of the group table of G.

$$\begin{array}{c|cccc} & & g_j & g_{j+1} & \\ \hline & & \cdots & \cdots & \\ g_{\pi(i)} & \cdots & g_{\pi(i)} g_j & g_{\pi(i)} g_{j+1} & \cdots \\ g_{\pi(i+1)} & \cdots & g_{\pi(i+1)} g_j & g_{\pi(i+1)} g_{j+1} & \cdots \\ & & \cdots & \cdots & \end{array}$$

Then the equivalencies follow from (1) and (2):

(1) $g_{\pi(i)} g_j = g_{\pi(i+1)} g_{j+1} \iff g_{\pi(i)}^{-1} g_{\pi(i+1)} = g_j g_{j+1}^{-1}$
(2) $g_{\pi(i)} g_{j+1} = g_{\pi(i+1)} g_j \iff g_{\pi(i)}^{-1} g_{\pi(i+1)} = g_{j+1} g_j^{-1}$. □

Now we can state equivalent conditions for two rows of the group table to have cyclically different entries in diagonally adjacent positions and for the Lohse form of the group table.

Corollary 1. *Let G be a group of order n with group table $g_{i,j} = g_{\pi(i)} g_j$ as in Lemma 1.*

Then (1) *and* (2) *are equivalent:*

(1) *Rows r_i and r_{i+1} of the group table have cyclically different entries in diagonally adjacent positions.*
(2) $g_{\pi(i)}^{-1} g_{\pi(i+1)} \notin Q(h^{-1})$.

Proof. By Lemma 1(a2) and (b2) rows r_i and r_{i+1} of the group table have cyclically different entries in diagonally adjacent positions if and only if $g_{\pi(i)}^{-1} g_{\pi(i+1)} \neq g_j g_{j+1}^{-1}$ for $0 \le j < n$ and $g_{\pi(i)}^{-1} g_{\pi(i+1)} \neq g_{j+1} g_j^{-1}$ for $0 \le j < n$. The elements $g_j g_{j+1}^{-1}$ and $g_{j+1} g_j^{-1}$ for $0 \le j < n$ are precisely the elements of $Q(h^{-1})$ and therefore the equivalence of (1) and (2) follows. □

Corollary 2. *Let G be a group of order n with group table $g_{i,j} = g_{\pi(i)} g_j$ as in Lemma 1.*

Then (1) *and* (2) *are equivalent:*

(1) *The group table is in Lohse form.*
(2) $Q(h^{-1}) \cap Q(v) = \emptyset$.

Proof. By Lemma 1(a2) and (b2) the group is in Lohse form if and only if $g_{\pi(i)}^{-1} g_{\pi(i+1)} \neq g_j g_{j+1}^{-1}$ for $0 \le i, j < n$ and $g_{\pi(i)}^{-1} g_{\pi(i+1)} \neq g_{j+1} g_j^{-1}$ for $0 \le i, j < n$. The elements

$g_{\pi(i)}^{-1} g_{\pi(i+1)}$ are in $Q(v)$ and the elements $g_j g_{j+1}^{-1}$ and $g_{j+1} g_j^{-1}$ with $0 \le j < n$ are precisely the elements of $Q(h^{-1})$. The equivalence of (1) and (2) follows now since $Q(h^{-1})$ is closed under taking inverses and $Q(v)$ consists of the elements $g_{\pi(i)}^{-1} g_{\pi(i+1)}$ for $0 \le i < n$ and their inverses. □

Since the inverse of an enumeration of the elements of a group G is again an enumeration of the elements, we get from the equivalence of (1) with (2) of Corollary 2 the next theorem.

Theorem 1. *The group G has the Lohse property if and only if it has two enumerations of its elements $e_1 = (g_{1,0}, g_{1,1}, \ldots, g_{1,n-1})$ and $e_2 = (g_{2,0}, g_{2,1}, \ldots, g_{2,n-1})$ such that $Q(e_1) \cap Q(e_2) = \emptyset$.*

It is this criterion that we use in the rest of the paper. The group table in Lohse form is constructed from the two enumerations $e_1 = (g_{1,0}, g_{1,1}, \ldots, g_{1,n-1})$ and $e_2 = (g_{2,0}, g_{2,1}, \ldots, g_{2,n-1})$ by taking one of the two enumerations as vertical border and the inverse of the other as horizontal border of the multiplication table and forming the products.

We end this section with two simple observations.

Proposition 1. (a) *If $e = (g_0, g_1, \ldots, g_{n-1})$ is an enumeration of the elements of the group G, then $Q(e)$ is a generating system of G.*

(b) *If there exists an enumeration $e = (g_0, g_1, \ldots, g_{n-1})$ of the elements of G such that $|Q(e)| \le |G| - 2$, then we can find a group table of G that has two rows r_i and r_{i+1} with cyclically different entries in diagonally adjacent positions.*

Proof. (a) This follows since the identity element 1 is in the enumeration and the consecutive quotients are in $Q(e)$.

(b) Let $g \neq 1$ be an element of G not in $Q(e)$. Then the first two rows of group table with $h = (g_0^{-1}, g_1^{-1}, \ldots, g_{n-1}^{-1})$ as horizontal border and $v = (1, g, \ldots)$ as vertical border satisfy (2) of Corollary 1. □

3. Groups that do not have the Lohse property

We show that the quaternion group is not a Lohse group. It is easy to see that there are no 2×2, 3×3 and 4×4 latin squares with the Lohse property. Therefore groups of order 2, 3 and 4 do not have the Lohse property. For later use we show first that, for groups of order four, we can find a Cayley table with two rows that have cyclically different entries in diagonally adjacent positions.

Lemma 2. *There are two non-isomorphic groups of order four, the cyclic group of order four $C_4 = \{1, a, a^2, a^3\}$ and the elementary abelian two-group $V_4 = \{(1, 1), (1, a), (a, a), (a, 1)\}$ with elementwise multiplication and $a^2 = 1$. Both have an enumeration e of the elements with $Q(e) \le |G| - 2$ and therefore, by Proposition 1(b), both have a group table in which there exist two rows that have cyclically different entries in diagonally adjacent positions.*

Proof. For the group C_4 the enumeration $e = (1, a, a^2, a^3)$ has $Q(e) = \{a, a^3\}$ and does not contain a^2. For group V_4 the enumeration $e = ((1, 1), (1, a), (a, a), (a, 1))$ has $Q(e) = \{(1, a), (a, 1)\}$ and does not contain (a, a). □

Lemma 3. *The quaternion group does not have the Lohse property.*

Proof. The quaternion group Q is the group with the following group table:

	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	$-i$	1	$-k$	j
j	j	$-k$	-1	i	$-j$	k	1	$-i$
k	k	j	$-i$	-1	$-k$	$-j$	i	1
-1	-1	$-i$	$-j$	$-k$	1	i	j	k
$-i$	$-i$	1	$-k$	j	i	-1	k	$-j$
$-j$	$-j$	k	1	$-i$	j	$-k$	-1	i
$-k$	$-k$	$-j$	i	1	k	j	$-i$	-1

Every generating system closed under taking inverses of Q contains at least two of i, j, k; therefore, there do not exist $e_1 = (g_{1,0}, g_{1,1}, \ldots, g_{1,7})$ and $e_2 = (g_{2,0}, g_{2,1}, \ldots, g_{2,7})$ such that $Q(e_1) \cap Q(e_2) = \emptyset$. □

4. Cyclic, dihedral, dicyclic groups and $C_3 \times C_3$

We show that cyclic, dihedral, dicyclic groups and $C_3 \times C_3$ are Lohse groups by constructing two enumerations e_1 and e_2 with $Q(e_1) \cap Q(e_2) = \emptyset$.

Lemma 4. *If G is a cyclic group of order greater than four, then G has the Lohse property.*

Proof. (a) If $G = \langle c \rangle$ is of odd order, then let $e_1 = (1, c, c^2, \ldots, c^{n-1})$ and $e_2 = (1, c^2, c^4, \ldots, c^{n-1}, c, c^3, \ldots, c^{n-2})$. Then $Q(e_1) = \{c, c^{-1}\}$ and $Q(e_2) = \{c^2, c^{-2}\}$ and for $n > 4$ this implies $Q(e_1) \cap Q(e_2) = \emptyset$.

(b) If $G = \langle c \rangle$ is of even order, then let $e_1 = (1, c, c^2, \ldots, c^{n-1})$ and $e_2 = (1, c^2, c^4, \ldots, c^{n-2}, c, c^{n-1}, c^{n-3}, \ldots, c^3)$. Then $Q(e_1) = \{c, c^{n-1}\}$ and $Q(e_2) = \{c^2, c^3, c^{-2}, c^{-3}\}$ and for $n \geq 6$ this implies $Q(e_1) \cap Q(e_2) = \emptyset$. □

Lemma 5. *The dihedral group G of order $2n$ is the group with the presentation*

$$G = \langle a, b | a^n = 1 = b^2, b^{-1}ab = a^{-1} \rangle.$$

If n is greater than two, then G has the Lohse property.

Proof. Let $e_1 = (1, a, a^2, \ldots, a^{n-1}, b, ba, ba^2, \ldots, ba^{n-1})$ and $e_2 = (1, b, a, ab, a^2, a^2b, \ldots, a^{n-1}, a^{n-1}b)$. Then $Q(e_1) = \{a, a^{-1}, ba^{-1}\}$ and $Q(e_2) = \{b, ba\}$. Therefore $Q(e_1) \cap Q(e_2) = \emptyset$ for $n > 2$. □

Lemma 6. *The dicyclic group G of order $2n$ with $n = 2m$ is the group that has the presentation*

$$G = \langle a, b | a^{2m} = 1, b^2 = a^m, b^{-1}ab = a^{-1} \rangle.$$

For m greater than two, G has the Lohse property.

Proof. Let $e_1 = (1, a, a^2, \ldots, a^{n-1}, b, ba, ba^2, \ldots, ba^{n-1})$ and $e_2 = (1, b, a, ab, a^2, a^2b, \ldots, a^{n-1}, a^{n-1}b)$. Then $Q(e_1) = \{a, a^{-1}, ab, b^{-1}a^{-1}, ba^{-1}, ab^{-1}\} = \{a, a^{-1}, ba^{-1}, ba^{m-1}\}$ and $Q(e_2) = \{b, b^{-1}, b^{-1}a, ba\} = \{b, ba^m, ba^{m+1}, ba\}$ and therefore for $m > 2$ we get $Q(e_1) \cap Q(e_2) = \emptyset$. $\square$

Lemma 7. *The direct product of two groups of order 3, the group $C_3 \times C_3$, has the Lohse property.*

Proof. If we set $e_1 = ((1, 1), (1, a), (1, a^2), (a, 1), (a, a), (a, a^2), (a^2, 1), (a^2, a), (a^2, a^2))$ and $e_2 = ((1, 1), (a, a^2), (1, a^2), (a^2, a^2), (1, a), (a, 1), (a^2, 1), (a, a), (a^2, a))$ we get $Q(e_1) = \{(1, a), (1, a^2), (a, a), (a^2, a^2)\}$ and $Q(e_2) = \{(a, a^2), (a^2, a), (a, 1), (a^2, 1)\}$ and therefore $Q(e_1) \cap Q(e_2) = \emptyset$. $\square$

5. Building up larger groups from smaller groups

The main results of the section are the following. If the group G has a quotient Q which is a Lohse group, then it is itself a Lohse group. If G is a semidirect product AB, where $\{1\} \neq A$ is normal in G and B has a group table with two rows that have cyclically different entries in diagonally adjacent positions, then G is a Lohse group. The theorem from which we derive the result is more general. It is interesting to note that the structure of the normal subgroup plays in both cases no role.

Theorem 2. *Let A and B be subgroups of a group G, $A \cap B = \{1\}$, $G = AB$. If $|A| = n > 1$, and $1 \neq b \in B \cap N_G(A)$, where $N_G(A)$ denotes the normalizer of A in G, and there exists an enumeration $e_B = (b_0, b_1, \ldots, b_{m-1})$ of the elements of B such that $b \notin Q(e_B)$, then G has the Lohse property.*

Proof. With $A = \{a_0, a_1, \ldots, a_{n-1}\}$ we set $e_1 = (b_0a_0, \ldots, b_0a_{n-1}, b_1a_0, \ldots, b_1a_{n-1}, \ldots, b_{m-1}a_0, \ldots, b_{m-1}a_{n-1})$ and $e_2 = (a_0b_{\rho(0)}, a_0b_{\rho(1)}, \ldots, a_0b_{\rho(m-1)}, a_1b_{\rho(0)}, \ldots, a_1b_{\rho(m-1)}, \ldots, a_{n-1}b_{\rho(0)}, \ldots, a_{n-1}b_{\rho(m-1)})$, where $a_0 = 1$ and ρ is a permutation of $0, 1, \ldots, m-1$ such that $b_{\rho(0)} = 1$ and $b_{\rho(m-1)} = b$. Then $Q(e_1)$ consists of the distinct elements of $a_i^{-1}a_{i+1}$ for $0 \leq i < n-1$ and $a_{n-1}^{-1}b_i^{-1}b_{i+1}a_0$ for $0 \leq i < m$ and their inverses. Since $a_0 = 1$, the set $Q(e_1)$ consists of the distinct elements of $a_i^{-1}a_{i+1}$ for $0 \leq i < n-1$, $a_{n-1}^{-1}b_i^{-1}b_{i+1}$ for $0 \leq i < m$ and their inverses and $Q(e_2)$ consists of the distinct elements of $b_{\rho(i)}^{-1}b_{\rho(i+1)}$ for $0 \leq i < m-1$ and $b_{\rho(m-1)}^{-1}a_i^{-1}a_{i+1}b_{\rho(0)}$ for $0 \leq i < n$ and their inverses. Since $b_{\rho(0)} = 1$ and $b_{\rho(m-1)} = b$, the set $Q(e_2)$ consists of the distinct elements of $b_{\rho(i)}^{-1}b_{\rho(i+1)}$ for $0 \leq i < m-1$ and $b^{-1}a_i^{-1}a_{i+1}$ for $0 \leq i < n$ and their inverses.

We show that none of the elements of $Q(e_2)$ is in $Q(e_1)$. Since $Q(e_2)$ contains with every element its inverse, it is enough to show that none of $b_{\rho(i)}^{-1}b_{\rho(i+1)}$ for $0 \leq i < m-1$, of $b^{-1}a_i^{-1}a_{i+1}$ for $0 \leq i < n$ is in $Q(e_1)$. From $|A| > 1$ we conclude that $a_{n-1} \neq 1$, such that the elements $b_{\rho(i)}^{-1}b_{\rho(i+1)}$ for $0 \leq i < m-1$ are not in $Q(e_1)$. Also since $b \neq 1$, the elements of $b^{-1}a_i^{-1}a_{i+1}$ for $0 \leq i < n$ are not in A. It is therefore enough to show that the elements of $b^{-1}a_i^{-1}a_{i+1}$ for $0 \leq i < n$ are different from the elements $a_{n-1}^{-1}b_i^{-1}b_{i+1}$ for $0 \leq i < m$ and their inverses. Now b is not in the set of the distinct elements of $b_i^{-1}b_{i+1}$ for $0 \leq i < m$ and their inverses, and therefore, since $A \cap B = \{1\}$, an element of the form $b^{-1}a_i^{-1}a_{i+1}$ is different from an inverse of $a_{n-1}^{-1}b_i^{-1}b_{i+1}$ for $0 \leq i < m$. On the other hand, $b^{-1}a_i^{-1}a_{i+1} = a_i'b^{-1}$ for some element a_i' of A since $b \in N_G(A)$. Therefore an element of the form $b^{-1}a_i^{-1}a_{i+1}$ is different from $a_{n-1}^{-1}b_i^{-1}b_{i+1}$ for $0 \leq i < m$. □

Corollary 3. *Let G be the semidirect product of the normal subgroup A and the subgroup B. If $|A| > 1$, and $1 \neq b \in B$ and there exists an enumeration $e_B = (b_0, b_1, \ldots, b_{m-1})$ of the elements of B such that $b \notin Q(e_B)$, then G has the Lohse property.*

As an application we show that an abelian group is a Lohse group.

Proposition 2. *If G is abelian and $|G| > 4$, then G has the Lohse property.*

Proof. G can be decomposed into a direct product of cyclic groups $G = C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k}$ with the additional property that $n_i > 1$ and n_i is a divisor of n_{i+1} for $1 \leq i < k$; see for example in [7].

(a) $k = 1$. Then G is cyclic and of order greater than four and therefore by Lemma 4 a Lohse group.
(b) $k > 1, n_k \geq 4$. Let $A = C_{n_1} \times C_{n_2} \times \cdots \times C_{n_{k-1}}$ and $B = C_{n_k}$. If $n_k > 4$, then B is a Lohse group and has therefore an enumeration $e_B = (b_0, b_1, \ldots, b_{m-1})$ of the elements of B such that there exists $1 \neq b \notin Q(e_B)$. In Lemma 2 this is also shown for $B = C_4$. The prerequisites of Corollary 3 are therefore satisfied and G is a Lohse group.
(c) $k > 1, n_k = 3$. Then G is an elementary abelian 3-group. Since $|G| > 4$, we get that either $G = C_3 \times C_3$, and this is a Lohse group by Lemma 7, or G contains the Lohse group $C_3 \times C_3$ as a direct factor and is a Lohse group by Corollary 3.
(d) $k > 1, n_k = 2$. Then G is an elementary abelian 2-group. Since $|G| > 4$, we get that G contains $V_4 = C_2 \times C_2$ as a direct factor. In Lemma 2 it is shown that $B = V_4$ has an enumeration $e_B = (b_0, b_1, \ldots, b_{m-1})$ of the elements such that there exists $1 \neq b \notin Q(e_B)$; again by Corollary 3 the group G is therefore a Lohse group. □

Theorem 3. *Let G be a group with normal subgroup N and quotient group G/N. Then G/N is a Lohse group implies that G is a Lohse group.*

Proof. Let $\phi : G \to G/N$ be the projection map and $e_1(G/N) = (q_0, \ldots, q_{n-1})$ and $e_2(G/N) = (q_{\rho(0)}, \ldots, q_{\rho(n-1)})$, where ρ is a permutation of $0, 1, \ldots, n-1$, two enumerations of the elements of G/N with $Q(e_1(G/N)) \cap Q(e_2(G/N)) = \emptyset$. Let $p_i, i = 0, \ldots, n-1$ be elements of G such that $\phi(p_i) = q_i$ for $i = 0, \ldots, n-1$ and $b_0, b_1, \ldots, b_{m-1}$ the elements of N. Now we set

$$e_1 = (p_0b_0, \ldots, p_0b_{m-1}, p_1b_0, \ldots, p_1b_{m-1}, \ldots, p_{n-1}b_0, \ldots, p_{n-1}b_{m-1})$$

and

$$e_2 = (b_0p_{\rho(0)}, \ldots, b_0p_{\rho(n-1)}, \ldots, b_{m-1}p_{\rho(0)}, \ldots, b_{m-1}p_{\rho(n-1)}).$$

Then $Q(e_1)$ consists of the distinct elements of $b_i b_{i+1}^{-1}$ for $0 \le i < m-1$ and $b_{m-1}^{-1} p_i^{-1} p_{i+1} b_0$ for $0 \le i < n$ and their inverses. $Q(e_2)$ consists of the distinct elements of $p_{\rho(i)}^{-1} p_{\rho(i+1)}$ for $0 \le i < n-1$ and $p_{\rho(n-1)}^{-1} b_i^{-1} b_{i+1} p_{\rho(0)}$ for $0 \le i < m$ and their inverses. Now $\phi(Q(e_1)) \subseteq (Q(e_1(G/N)) \cup \{1_{G/N}\})$ and $\phi(Q(e_2)) \subseteq Q(e_2(G/N))$. Since $1_{G/N} \notin Q(e_2(G/N))$, it follows from $Q(e_1(G/N)) \cap Q(e_2(G/N)) = \emptyset$ that $\phi(Q(e_1)) \cap \phi(Q(e_2)) = \emptyset$, and therefore that $Q(e_1) \cap Q(e_2) = \emptyset$. □

6. Groups of order 8, 12, 16 and small multiples of 5

We apply the results of the previous sections to show that groups of order 12, 16 and small multiples of 5 are Lohse groups. First we prove a result on groups of order 8 that is used in the next section.

Lemma 8. *Groups of order 8 have an enumeration e with $|Q(e)| \le 4$.*

Proof. There are 5 non-isomorphic groups of order 8, three abelian groups, the dihedral group D_4 and the quaternion group Q.

C_8: By Lemma 4 there exists an enumeration e with $|Q(e)| = 2$.

$C_2 \times C_4$: Then $e = ((0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3))$ has $Q(e) = \{(0,1), (0,3), (1,1), (1,3)\}$.

$C_2 \times C_2 \times C_2$: Then $e = ((0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1))$ has $Q(e) = \{(0,0,1), (0,1,1), (1,1,1)\}$.

D_4: By Lemma 5 there exists an enumeration e with $|Q(e)| = 3$.

Q: The enumeration $e = (1, i, j, k, -1, -i, -j, -k)$ has $Q(e) = \{i, k, -i, -k\}$. □

Lemma 9. *Groups of order 12 are Lohse groups.*

Proof. A group of order 12 is abelian, dihedral, the alternating group A_4 or dicyclic; see [8]. By Proposition 2, Lemmas 5 and 6, we know that abelian, dihedral and dicyclic groups of order 12 are Lohse groups. It remains therefore to show that A_4 is a Lohse group. A_4 has a normal subgroup $C_2 \times C_2 = ((0,0), (0,1), (1,0), (1,1))$ on which an element a operates by cyclically permuting the three non-trivial elements $(1,0)^a = (0,1)$, $(0,1)^a = (1,1)$.

Let now $e_1 = ((0,0), (0,1), (1,0), (1,1), a(0,0), a(0,1), a(1,0), a(1,1), a^2(0,0), a^2(0,1), a^2(1,0), a^2(1,1))$ and $e_2 = ((0,0), (0,0)a, (0,0)a^2, (0,1), (0,1)a, (0,1)a^2, (1,0), (1,0)a, (1,0)a^2, (1,1), (1,1)a, (1,1)a^2)$ then $Q(e_1) = \{(0,1), (1,1), (1,1)a, a^2(1,1)\} = \{(0,1), (1,1), a(1,0), a^2(1,1)\}$ and $Q(e_2) = \{a, a^2, a(0,1), a(1,1), (0,1)a^2, (1,1)a^2\} = \{a, a^2, a(0,1), a(1,1), a^2(1,0), a^2(0,1)\}$ and therefore $Q(e_1) \cap Q(e_2) = \emptyset$. □

Lemma 10. *Groups of order 16 are Lohse groups.*

Proof. According to [8], there are 14 non-isomorphic groups of order 16. We follow the enumeration in [8]. The first five groups are abelian and therefore Lohse groups by Proposition 2.

Group G_6 is isomorphic to $D_4 \times C_2$. Since D_4, the dihedral group of order 8, is a Lohse group by Lemma 5, we can apply Corollary 3 to derive that group G_6 is a Lohse group.

Group G_7 is isomorphic to $Q \times C_2$ where Q is the quaternion group. By Lemma 8 the quaternion group has an enumeration e with $|Q(e)| \leq 4$, the assumptions of Corollary 3 hold and G_7 is therefore a Lohse group.

Group $G_8 = \langle a, b, c | a^2 = 1, b^2 = 1, c^2 = 1, abc = bca = cab \rangle$ and $G_9 = \langle a, b | a^4 = 1, b^4 = 1, (ab)^4 = 1, (a^{-1}b)^4 = 1 \rangle$. For both groups, the abelian quotients G_{8ab} and G_{9ab} are of order 8 and therefore Lohse groups by Proposition 2 so that by Theorem 3 the groups G_8 and G_9 are Lohse groups.

Group $G_{10} = \langle a, b | a^4 = 1, b^4 = 1, a^{-1}ba = b^{-1} \rangle$ is a semidirect product of cyclic group of order 4 with a cyclic group of order 4 and therefore, by Lemma 2 and Corollary 3, a Lohse group.

Group $G_{11} = \langle a, b | a^8 = 1, b^2 = 1, b^{-1}ab = a^5 \rangle$. The abelian quotient G_{11ab} is of order 8 and therefore a Lohse group by Proposition 2 so that by Theorem 3 the group G_{11} is a Lohse group.

Group G_{12} is the dihedral group of order 16 and therefore a Lohse group by Lemma 5.

Group $G_{13} = \langle a, b | a^8 = 1, b^2 = 1, b^{-1}ab = a^3 \rangle$. The element a^4 is in the centre of G_{13} and the quotient group $G_{13}/\langle a^4 \rangle$ is the dihedral group of order 8 which is a Lohse group by Lemma 5 and by Theorem 3 the group G_{13} is a Lohse group.

Group G_{14} is the dicyclic group of order 16 and therefore a Lohse group by Lemma 6. □

Lemma 11. *Groups of order 5, 10, 15, 20 and 25 are Lohse groups.*

Proof. Groups of order 5 and 15 are cyclic and therefore Lohse groups by Lemma 4. Groups of order 10 are cyclic or dihedral, therefore Lohse groups by Lemmas 4 and 5. According to [8], groups of order 20 are abelian, dihedral, dicyclic or the semidirect product of a normal subgroup of order 5 with a group of order 4. The abelian, dihedral and dicyclic groups are Lohse groups by Proposition 2 and Lemmas 5 and 6. The semidirect product of a normal subgroup of order 5 with a group of order 4 is by Lemma 2 and Corollary 3 a Lohse group. Groups of order 25 are abelian and therefore Lohse groups by Proposition 2. □

7. Groups with cyclic subgroups of order greater than four

If $e = (g_0, g_1, \ldots, g_{n-1})$ is an enumeration of the elements of the group G, then it was shown in Proposition 1(a) that the set $Q(e)$ is a set of generators and their inverses of G. The undirected graph which has as its vertices the elements of G where two vertices u and v are connected if there exists $s \in Q(e)$ with $us = v$ is called the Cayley graph $C(G)$ of G with respect to the generating system $Q(e)$. In $C(G)$ the elements $g_0, g_1, \ldots, g_{n-1}$ form in this order a so-called Hamilton cycle. Conversely let S be a set of generators and their inverses, and $C(G)$ the Cayley graph of G with respect to S. If $C(G)$ contains a Hamilton cycle $g_{i_0}, g_{i_1}, \ldots, g_{i_{n-1}}$ then we get $Q(e) \subseteq S$ for the enumeration $e = (g_{i_0}, g_{i_1}, \ldots, g_{i_{n-1}})$. It is an open question if every Cayley graph of a group with respect to a generating system S contains a Hamilton cycle, see [1], but a well known theorem on graphs from Dirac, [3], says that a graph with $n \geq 3$ vertices where from each vertex there are at least $n/2$ edges always contains a Hamilton cycle. This gives us the following theorem.

Theorem 4. *If there exists an enumeration of the elements $e = (g_0, g_1, \dots, g_{n-1})$ for the group G with $|Q(e)| \leq |G|/2 - 1$, then G has the Lohse property.*

Proof. Let $S' = G - Q(e) - \{1\}$ (set difference), then $|S'| \geq |G|/2$. Note that S' is necessarily a generating system of G, because the subgroup generated by S', which contains in addition to S' at least also the 1 element, has more than $|G|/2$ elements and is therefore the whole group. Because $Q(e)$ contains with every element its inverse, S' does also. But by Dirac's theorem the Cayley graph contains now a Hamilton cycle $g_{i_0}, g_{i_1}, \dots, g_{i_{n-1}}$. The enumeration $e' = (g_{i_0}, g_{i_1}, \dots, g_{i_{n-1}})$ has $Q(e') \subseteq S'$, and therefore e and e' are two enumerations with $Q(e) \cap Q(e') = \emptyset$. $\square$

As an application we show that almost all groups are Lohse groups.

Theorem 5. *The following groups have the Lohse property:* (a) *Groups of order $|G| = pm$ with p a prime, $p > 5$.* (b) *Groups of order $|G| = 5m$ with $m > 5$.* (c) *Groups of order $|G| = 9m$.* (d) *Groups of order $|G| = 8m$ with $m > 2$.*

Proof. By the Cauchy and Sylow theorems, see for example in [7], the group G contains a subgroup U of order $p \geq 5$ or of order 9 or 8. Let $r_0, r_1, \dots, r_{m-1}$ be representatives of the right cosets of U.

(a)(b) Then with $U = \langle u \rangle$ we get for $e_U = (1, u, u^2, \dots, u^{p-1})$ that $Q(e_U) = \{u, u^{p-1}\}$. Let now $e = (r_0, r_0u, r_0u^2, \dots, r_0u^{p-1}, r_1, r_1u, \dots, r_1u^{p-1}, \dots, r_{m-1}, r_{m-1}u, \dots, r_{m-1}u^{p-1})$.

Then e is an enumeration of the elements of G and $Q(e)$ consists of the distinct elements of u and $ur_i^{-1}r_{i+1}$ for $i = 0, \dots, m-1$ and their inverses and therefore $|Q(e)| \leq 2 + 2m$.

To apply Theorem 4, we need that $|Q(e)| \leq |G|/2 - 1$. Now $2 + 2m \leq pm/2 - 1$ is equivalent to $6 \leq (p-4)m$.

(a) $p > 5$ and p a prime, then p is at least 7 and the inequality $6 \leq (p-4)m$ holds for $m \geq 2$. Groups with a cyclic subgroup of order $p \geq 7$ of index at least 2 are therefore Lohse groups, but by Lemma 4 also cyclic groups of order 7 and larger, so that (a) is complete.

(b) $p = 5$, then $6 \leq (p-4)m$ is equivalent with $6 \leq m$, therefore all groups of order $5m$ with $m > 5$ satisfy by Theorem 4 the Lohse property.

(c) $|G| = 9m$. Then the subgroup U of order 9 is either cyclic of order 9 or a direct product of two cyclic subgroups of order 3. A cyclic group has an enumeration e of the elements with $|Q(e)| \leq 2$ and by Lemma 7 the group $C_3 \times C_3$ has an enumeration e with $|Q(e)| \leq 4$. Therefore U has an enumeration $e_U = (u_0, u_1, \dots, u_8)$ with $|Q(e_U)| \leq 4$. Let $e = (r_0u_0, r_0u_1, r_0u_2, \dots, r_0u_8, r_1u_0, r_1u_1, \dots, r_1u_8, \dots, r_{m-1}u_0, r_{m-1}u_1, \dots, r_{m-1}u_8)$.

Then the consideration above shows that $|Q(e)| \leq 4 + 2m$ and $4 + 2m \leq 9m/2 - 1$ is equivalent to $10 \leq 5m$; therefore, by Theorem 4, groups with a subgroup of order 9 of index at least 2 are Lohse groups. But by Lemma 4 the cyclic group of order 9, and by Lemma 7 the group $C_3 \times C_3$, have the Lohse property, so that (c) is complete.

(d) $|G| = 8m$. By Lemma 8 the subgroup U of order 8 has an enumeration $e_U = (u_0, u_1, \dots, u_7)$ with $|Q(e_U)| \leq 4$. Let $e = (r_0u_0, r_0u_1, r_0u_2, \dots, r_0u_7, r_1u_0, r_1u_1, \dots, r_1u_7, \dots, r_{m-1}u_0, r_{m-1}u_1, \dots, r_{m-1}u_7)$.

Then the consideration above shows again that $|Q(e)| \leq 4+2m$ and $4+2m \leq 8m/2-1$ is equivalent to $5 \leq 2m$; therefore, groups with a subgroup of order 8 of index at least 3 have the Lohse property, so that (d) is complete. $\square$

Theorem 6. *A finite group has the Lohse property if and only if it is of order greater 4 and not isomorphic to the group of quaternions.*

Proof. The groups not covered by Theorem 5 belong to (a) $|G| = 5, 10, 15$ or 25, (b) $|G|$ is a divisor of 16 or (c) $|G|$ is a divisor of 12. These cases are treated in the previous sections. $\square$

Acknowledgement

I would like to thank the referee for his constructive comments to the paper which have improved its presentation.

References

[1] S.J. Curran, J.A. Gallian, Hamiltonian cycles and paths in Cayley graphs and digraphs—A survey, Discrete Math. 156 (1996) 1–18.
[2] J. Denes, A.D. Keedwell, Latin Squares and Their Applications, Akademiai Kiado, Budapest, 1974.
[3] G.A. Dirac, Some theorems on abstract graphs, Proc. London Math. Soc. 2 (1952) 69–81.
[4] E. Gomriger, F.W. Heckmanns et al., Richard Paul Lohse Modulare und Serielle Ordnungen, M. DuMont Schauberg, Koeln, 1973.
[5] A. Hedayat, A complete solution to the existence and nonexistence of Knut Vik designs and orthogonal Knut Vik designs, J. Combin. Theory Ser. A 22 (1977) 331–337.
[6] H.-P. Riese, F.W. Heckmanns, Richard Paul Lohse Zeichnungen Dessins 1935–1985, LIT Verlag, CH-Baden, 1986.
[7] J.J. Rotman, An Introduction to the Theory of Groups, Wm.C. Brown Publishers Dubuque, Iowa, 1988.
[8] A.D. Thomas, G.V. Wood, Group Tables, Shiva Publishing Ltd, Orpington, 1980.